Samuel M. Lasser (SBN – 252754)
slasser@edelson.com
EDELSON PC
1934 Divisadero Street
San Francisco, California 94115
Tel: 415.994.9930
Fax: 415.776.8047

Rafey S. Balabanian*
rbalabanian@edelson.com
Benjamin H. Richman*
brichman@edelson.com
J. Dominick Larry*
nlarry@edelson.com
Amir C. Missaghi*
amissaghi@edelson.com
EDELSON PC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

**Pro hac vice* admission to be sought.

Attorneys for Plaintiff and the Putative Class

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

DAVID HUNTER, individually, and on behalf of all others similarly situated,

Plaintiff,

v.

LENOVO (UNITED STATES), INC., a Delaware corporation, and SUPERFISH, INC., a Delaware corporation,

Defendants.

Case No.

CLASS ACTION COMPLAINT FOR:

1. **Violations of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq*.;**
2. **Violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2510–2522; and**
3. **Unjust Enrichment**

DEMAND FOR JURY TRIAL

Plaintiff David Hunter brings this Class Action Complaint ("Complaint") against Defendants Lenovo (United States), Inc. ("Lenovo") and Superfish, Inc., ("Superfish") (collectively, "Defendants") for their unauthorized infiltration and surveillance of millions of unsuspecting consumers' personal computers. Plaintiff, for his Complaint, alleges as follows upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

INTRODUCTION

1. Each year, millions of consumers buy computers from Lenovo, trusting the company to provide reliable, secure computers. Unfortunately, in September 2014, Lenovo betrayed that trust by partnering with Superfish—an aspiring leader in the "visual search engine" market—to install a monitoring application (the "Superfish Surveillance Software") on Lenovo computers sold to consumers.

2. The privacy implications of Defendants' Superfish Surveillance Software cannot be overstated. As an initial matter, Defendants install "root certificates"[1] on the affected computers to ensure unimpeded access to consumers' internet traffic. Defendants' root certificates were so poorly implemented, though, that they effectively bar consumers from securing *any* internet transaction—even after Defendants' software is removed.

3. Once Defendants have placed their root certificate on the computers, their Superfish Surveillance Software installs a program that reroutes consumers' internet traffic. A consumer's request to visit a website, for example, no longer heads straight to its destination; instead, Defendants' Superfish Surveillance Software intercepts the request, performs searches and analysis, endeavors to modify the contents, and then re-sends the request to the original destination.

4. Then, when the consumer's computer receives a response from a website's servers, Defendants' Superfish Surveillance Software intercepts that as well. Once intercepted, the Software forever alters the contents by injecting custom computer code into the response in an effort to display advertisements.

[1] "Root certificates" are more fully explained in ¶¶ 17-24 of this Complaint.

5. By installing and operating their Superfish Surveillance Software without consent, Defendants have violated the privacy rights of millions of individuals. In addition, the manner in which Defendants' Superfish Surveillance Software operates violates several federal laws that aim to protect consumers against such unauthorized access to their communications and computers.

6. Accordingly, Plaintiff Hunter, on his own behalf and on behalf of a Class of similarly situated individuals, brings this lawsuit seeking to compel Defendants to remove their Superfish Surveillance Software and root certificates from Plaintiff's and the Class's computers, as well as recover statutory and actual damages, costs, and attorneys' fees.

PARTIES

7. Plaintiff David Hunter is a natural person and citizen of the State of North Carolina.

8. Defendant Lenovo (United States), Inc., is a corporation existing under the laws of the State of Delaware with its principal place of business located at 1009 Think Place, Morrisville, North Carolina 27560. Lenovo does business throughout the United States, the State of California, and this District.

9. Defendant Superfish, Inc., is a corporation existing under the laws of the State of Delaware with its principal place of business located at 2595 East Bayshore Road, Palo Alto, California 94303. Superfish does business throughout the United States, the State of California, and this District.

JURISDICTION AND VENUE

10. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331. This Court has personal jurisdiction over Defendants because they reside in this District,[2] conduct business in this District, and the improper conduct alleged in this

[2] Defendant Lenovo operates a "Research and Product Development Center" within this District, located at 602 Charcot Avenue, San Jose, California 95131, that "function[s] as a developmental lab and corporate office." *Lenovo opens New Office in Silicon Valley News in , -November 06, 2013 - at Lenovo*, http://www.lenovocareers.com/en/news-and-events/career-news-description/lenovo-opens-new-office-in-silicon-valley--412?cntry=united-states (last visited Feb. 23, 2015).

Complaint occurred in or emanated from this District.

11. The Court has personal jurisdiction over Defendants and venue is proper in this District because the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated from California, and because Defendants transact significant amounts of business within this District, enter into consumer and business contracts here, and Defendant Superfish is headquartered in this District.

INTRADISTRICT ASSIGNMENT

12. Pursuant to Civil Local Rule 3-2(e), this case shall be assigned to the San Jose Division.

FACTUAL BACKGROUND

I. Lenovo Partners with Superfish to Surreptitiously Install Surveillance Software on Millions of Computers

13. Defendant Lenovo is a leading manufacturer and seller of consumer personal computers, selling millions of computers and laptops every year.

14. Defendant Superfish is a company that envisages itself being the premier provider of image-based search results. Superfish employs dozens of engineers and scientists that work to teach computers how to recognize objects, such as animals, shoes, or smartphones, within images.

15. In 2014, Defendants partnered to pre-install Superfish's software onto millions of Lenovo computers. Through that partnership, Defendants devised a system whereby they profited by monitoring, intercepting, and monetizing the communications of millions of consumers.[3] Unfortunately, none of the monitored consumers were ever aware of the Superfish Surveillance Software's very existence.

[3] According to Superfish's "Non-exclusive Software Distribution Agreement," Superfish enters into "Revenue Shar[ing]" partnerships with distributors. *Superfish Inc. ("Superfish") Non-Exclusive Software Distribution Agreement*, www.similarproducts.net/SuperfishWebsiteDistributionAgreementV6US.pdf (last visited Feb. 23, 2015). Ostensibly, Lenovo and Superfish entered into a similar agreement, where Lenovo, acting as the distributor, would receive "50%" of revenue generated "from redirections to alternate sites made by [the Superfish Surveillance Software] during each month." *Id.*

II. Defendants Modify Users' Computers and Reroute Their Internet Traffic Without Their Consent.

16. Prior to January 2015, neither Lenovo nor Superfish disclosed to consumers that the Superfish Surveillance Software would modify their computers and monitor their online activities, nor did the Defendants ever seek to (or actually) obtain consumers' consent before doing so. Indeed, immediately after the user completes the initial setup of Windows, Defendants' Superfish Surveillance Software installs a "root certificate" that puts users' private information at risk and a "local proxy," that, as explained in detail below, intercepts users' communications.

A. Defendants Install an Insecure Root Certificate.

17. On every Lenovo computer with the Superfish Surveillance Software installed, Defendants also installed a "root certificate" that eviscerates users' abilities to securely communicate over the internet.

18. In very basic terms, a root certificate is part of an intricate system that helps ensure that websites on the internet are secure. The Windows operating system comes pre-packaged with a store of root certificates issued by trustworthy Certificate Authorities such as VeriSign.[4]

19. A Certificate Authority, such as VeriSign, distributes certificates to trustworthy companies like Amazon.com. When an individual browses Amazon.com, the user's web browser identifies a certificate that was "signed" by VeriSign, and the individual is given assurance that the website (Amazon.com) is secure. Without this system, it would be extremely difficult, if not impossible, for users to verify which websites were secure and safe for the transmission of sensitive information, such as credit card and bank account numbers.

20. Certificate Authorities like VeriSign must follow stringent regulations to have their root certificate included in web browsers or operating systems. For example, Microsoft requires entities applying for root certificates to comply with rigorous guidelines delineated by the WebTrust for Certification Authorities program, which is sponsored by the American

[4] VeriSign is a company that specializes in, among other things, online security and digital certificates. To date, VeriSign is the largest provider of digital certificates.

Institute for Certified Public Accountants (AICPA).

21. To average users, the significance of a root certificate is most readily manifested by a small image of a padlock in the top left of a web browser that appears when conducting secure transactions over the internet. This image provides the individual with peace of mind that sensitive information can be transmitted to the website without interception by nefarious actors. However, because Defendants install their own root certificate (without following any guidelines), the image of the padlock appears unbroken even while the Superfish Surveillance Software intercepts and captures all secure communications.

22. To install their root certificate (the "Superfish Root Certificate"), Defendants utilize a product called the "Komodia SSL Digestor" that "allows the programmer [*i.e.*, Defendants] a transparent access to decrypted [secure internet traffic] … without raising an alert from the [user's] browser." Komodia, the seller of the Digestor, states that it is:

> "a modified Man In The Middle attack. what it does is 'talk' with the application [*e.g.*, an internet browser] on one side, and talking with the target server on the other [*e.g.,* Amazon.com's servers], and the [Digestor] being the man in the middle, just as someone who gets a secret whispered in each ear, normally the browser/app would raise an alert because of the modified certificate, but the [Digestor] installs a root [] certificate in advance which means the browser will not send an alert because the certificate created is legit from [the application's] point of view."

23. Just as Komodia described, Defendants' Superfish Surveillance Software and their Root Certificate creates a "Man In The Middle Attack," which is a well-known type of attack used by, amongst others, computer hackers,[5] spy agencies,[6] and foreign governments[7] to eavesdrop on private communications and steal confidential information.

24. Worse, Defendants designed their software to leave behind the Superfish Root

---

[5] *DoubleDirect: Hackers Redirect High-Traffic Sites Via New MITM Attack*, http://www.tripwire.com/state-of-security/latest-security-news/doubledirect-hackers-redirect-high-traffic-sites-using-new-man-in-the-middle-attack/ (last visited Feb. 23, 2015).

[6] *NSA disguised itself as Google to spy, say reports – CNET*, http://www.cnet.com/news/ nsa-disguised-itself-as-google-to-spy-say-reports/ (last visited Feb. 23, 2015).

[7] *Chinese government launches man-in-middle attack against iCloud [Updated] | Ars Technica*, http://arstechnica.com/security/2014/10/chinese-government-launches-man-in-middle-attack-against-icloud/ (last visited Feb. 23, 2015).

Certificate even after a monitored consumer uninstalls the Superfish Surveillance Software.[8] The risks caused by untrusted root certificates are well documented and Defendants' actions pose serious risks to monitored consumers' computer systems.[9]

25. For example, just days after the Superfish Surveillance Software was uncovered, a computer security expert publicly released a tool that "silently intercept[s] [secure] connections made from computers infected with Superfish malware" by exploiting Defendants' insecure root certificate.[10] Anyone using that tool at an airport, coffee shop, or another public place can eavesdrop on the confidential conversations of the potentially millions of consumers with the Superfish Surveillance Software still installed on their computers.

B. Defendants Install a "Local Proxy" to Reroute Internet Traffic.

26. After Defendants' Superfish Surveillance Software installs its root certificate, the software causes all of the user's internet traffic to pass through a "local proxy," which is a computer program that changes the destination of all outbound internet traffic and initially receives all in-bound internet traffic. That is, a computer with a local proxy running will have a request to Amazon.com initially pass through the local proxy before it reaches the original

---

[8] After public condemnation, Lenovo released an automated tool that purportedly removes the Superfish Surveillance Software from infected computers. *Lenovo Newsroom | Updated Lenovo Statement on Superfish*, http://news.lenovo.com/article_display.cfm?article_id=1931&view_id=1431& (last visited Feb. 23, 2015). However, Lenovo's tool does not remove the Superfish Surveillance Software from infected computers' "recovery disk." The recovery disk is provided by Lenovo to act as a backup of the Windows operating system in case a user suffers a critical failure or seeks to install a fresh installation of Windows. As a result, should Plaintiff or members of the putative Class actually use the recovery disk, the Superfish Surveillance Software will once again infect their computers.

[9] Hackers use untrusted root certificates such as Defendants' Superfish Root Certificate to intercept personal data from users without detection. Because the consumer mistakenly believes that the transaction is secure, he or she assumes that it is safe to input sensitive financial or other information. Armed with the "key" to Defendants' Superfish Root Certificate, a hacker can create the faux appearance of a secure transaction. Defendants, as the Superfish Root Certificate's authors know the key, but, and perhaps more troubling, the key Defendants chose was simply the word "komodia." Accordingly, the prospect that Defendants (or anyone else) may attempt to utilize the root certificates they have intentionally left behind on monitored consumers' computers is a very real threat.

[10] *0xPoly/Superphish · GitHub*, https://github.com/0xPoly/Superphish (last visited Feb. 23, 2015); *see also Errata Security: Exploiting the Superfish certificate*, http://blog.erratasec.com/2015/02/exploiting-superfish-certificate.html#.VOqBqlPF87N (last visited Feb. 23, 2015).

destination of Amazon.com's servers.

27. Defendants' local proxy is their version of a product sold by non-party Komodia, which is marketed as a "redirector product" ("Komodia Redirector"). The Komodia Redirector lets Defendants "redirect [] traffic" away from the user's intended recipient and "to the proxy service."[11] "When a connection is made" by the user, the Komodia Redirector determines whether a specific communication "should be intercepted" and then intercepts and reroutes the communications to the local proxy.[12]

28. Analyzing the Superfish Surveillance Software reveals that Defendants purchased the Komodia Redirector and integrated it into their Superfish Surveillance Software. And because Defendants previously installed the root certificate onto every affected Lenovo laptop, the Superfish Surveillance Software can (and does) read and alter the contents of the intercepted communications.

III. Defendants' Superfish Surveillance Software Reads and Alters the Contents of Consumers' Rerouted Internet Traffic.

A. Defendants Acquire the Contents of Consumers' Communications.

29. Defendants' claimed purpose of pre-installing the Superfish Surveillance Software on consumers' computers was to "to assist customers with discovering products similar to what they are viewing."[13] To provide that "assistance," the Superfish Surveillance Software obtains access to consumers' browsing sessions, determines what, if anything, the consumer is viewing, and communicates with Defendants' servers to offer the "similar" products that consumers can "discover."

30. The method by which Superfish Surveillance Software obtains access to consumers browsing sessions is described in Section II above. And once the Superfish Surveillance Software establishes the "man-in-the-middle attack," Defendants are in a position to view a consumer's online browsing and communication activity and to determine

---

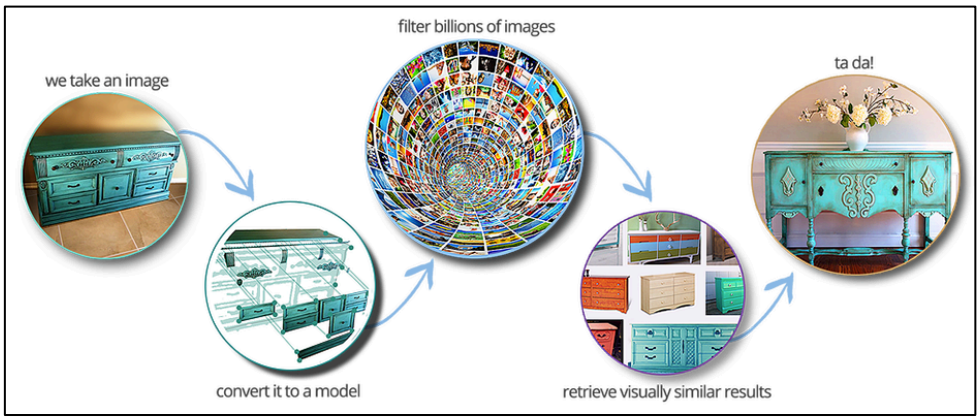
[11] *Komodia's Redirector – Komodia*, https://web.archive.org/web/20140807112859/http://www.komodia.com/wiki/index.php/Komodia%27s_Redirector (last visited Feb. 23, 2015).

[12] *Id.*

[13] *Superfish Vulnerability - Lenovo Support (US)*, http://support.lenovo.com/us/en/product_security/superfish (last visited Feb. 23, 2015).

what product, if any, the consumer is looking at.

31. Defendant Superfish describes its process for determining what consumers are looking at as first "tak[ing] an image," "convert[ing] it to a model," "filter[ing] billions of images," "retriev[ing] visually similar results," and then presenting the most similar product to the user:



(Figure 1.)[14]

The process outlined in Figure 1 occurs, in part, on the user's computer and also on Defendants' servers. The Superfish Surveillance Software continuously communicates with Defendants' servers to, among other things, "filter" and "retrieve visually similar results."

32. Defendants also use the millions of instances of the Superfish Surveillance Software to collect a vast amount of information about consumers and their internet browsing habits. According to Superfish's public statements, the Superfish Surveillance Software collects "usage data, referring/exit pages and URLs, platform types, number of clicks, etc."[15] Superfish then conducts "data mining"[16] to identify trends, habits, and patterns in consumers' browsing.

33. According to the terms of Superfish's standard distribution agreement,

---

[14] *About Us | SimilarProducts - Monetize Visually*, http://www.similarproducts.net/about-us/ (last visited Feb. 23, 2015) (describing Defendant Superfish's functionally equivalent "SimilarProducts" product which may be incorporated in whole or in part in Defendants' Superfish Surveillance Software).

[15] *Privacy Policy | SimilarProducts - Monetize Visually*, http://www.similarproducts.net/ privacy-policy/ (last visited Feb. 23, 2015).

[16] *Michael Chertok | ZoomInfo.com*, http://www.zoominfo.com/p/Michael-Chertok/1433596671 (reprinting that Defendant Superfish's Chief Technology Officer, Michael Chertok, has "10 years of experience in building large scale real-time data mining systems.").

Defendants developed "an identifying electronic signature that [] contain[s] DLsource and UserID that [] enable[s] Superfish to track installations and un-installations of the App, searches and merchant clicks."[17] The plethora of consumer information collected by the Superfish Surveillance Software and analyzed by Superfish is valuable to Defendants because they can sell or exchange the collected data to or with "interested third parties."[18]

B. Defendants Alter the Contents of Consumers' Communications.

34. As described above, Defendants' implementation of the Komodia Redirector decrypts all encrypted data so that the Superfish Surveillance Software can read the contents of the communications. Once the Superfish Surveillance Software has processed the contents, Defendants' Komodia Redirector encrypts the data once again to ensure that the receiving server (the indented recipient of the original communication) receives an encrypted communication as expected. The same decryption-encryption process occurs in reverse when the infected computer receives secure communications.

35. As such, any communication made or received by an infected computer is always altered. Specifically, Defendants' Superfish Surveillance Software replaces a user's default root certificate (that was securely signed by a trusted source) with the Superfish Root Certificate (which, conversely, is completely insecure and untrusted), forever changing all communications originated from users' computers. Moreover, all communication is decrypted before it reaches its intended recipient, another wholesale modification.

36. In addition, Defendants' Superfish Surveillance Software seeks to inject custom computer code into users' browsing sessions to display advertisements. After the Superfish Surveillance Software obtains access to a user's communications and determines what product (if any) a consumer is looking at, it transmits information to Superfish's servers and receives a list of similar products to advertise to the user. The Superfish Surveillance Software then "injects" bespoke computer code to display the advertisements on any website

[17] *Superfish Inc. ("Superfish") Non-exclusive Software Distribution Agreement*, http://www.similarproducts.net/SuperfishWebsiteDistributionAgreementV6US.pdf (last visited Feb. 23, 2015).

[18] *Privacy Policy | SimilarProducts - Monetize Visually*, www.similarproducts.net/privacy-policy/ (last visited Feb. 23, 2015).

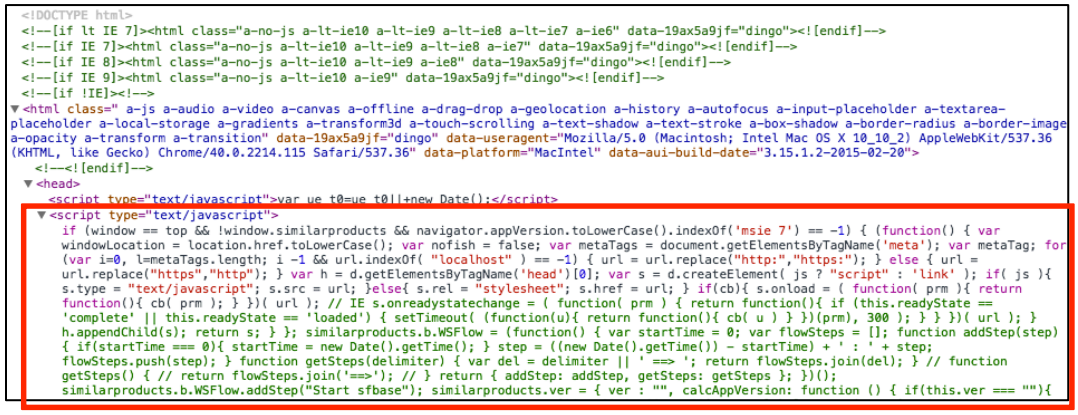
viewed by the user.

37. For example, when a website, such as Amazon.com, transmits computer code to a user's computer to facilitate online shopping, the code and accompanying files are temporarily stored before, during, and a short time after the user views and interacts with the site. But in the time before the user views the website, and while the code is temporarily stored, the Superfish Surveillance Software executes its injection function to modify the code.

38. Figure 2, shows a portion of the source code for Amazon.com that facilitates the operation of the website. In this example, the Superfish Surveillance Software has not injected any of Defendants' code.

(**Figure 2.**)

39. Figure 3, shows the same code from Amazon.com and demonstrates how just some of Defendants' code is injected, which is highlighted by a red box.



(**Figure 3.**)

40. The result of the injected computer code is similar to what is shown in Figure 4. In that case, the user is looking at shoes, and the Superfish Surveillance Software's code causes a "pop-up" "WindowShopper" box to appear showing eight similar shoes available

for purchase online. Per the likely terms of Defendants' agreement, had the consumer purchased one of the recommended similar shoes, each Defendant would profit.

(**Figure 4.**)[19]

IV. Computer Security Experts and Government Officials Discover Defendants' Superfish Surveillance Software and are Outraged.

41. It was not until January 23, 2015 that Lenovo, after receiving consumer complaints, confirmed that it had installed the Superfish Surveillance Software on certain of its laptops.[20] Lenovo stated at the time:

> "Due to some issues (browser pop up behavior for example), with the Superfish Visual Discovery browser add-on, we have temporarily removed Superfish from our consumer systems until such time as Superfish is able to provide a software build that addresses these issues. As for units already in market, we have requested that Superfish auto-update a fix that addresses these issues."

42. Just weeks later, Lenovo updated its response because the situation apparently "evolved." Lenovo pointed consumers to a "Lenovo Security Advisory" that stated that the "SUPERFISH VULNERABILITY" Defendants had installed on millions of computers was, in truth, a "Man-in-the-Middle Attack" of "High" "Severity."[21]

43. Since then, computer security experts have explained why Defendants' scheme was bad from the start. One stated that:

---

[19] *Visual Search for your Toolbar or Add-on | SimilarProducts - Monetize Visually*, http://www.similarproducts.net/enroll/ (last visited Feb. 23, 2015) (showing the result of injected computer code created by Defendant Superfish's "WindowShopper" program that is functionally equivalent to Defendants' Superfish Surveillance Software.)

[20] *Id.*

[21] *Superfish Vulnerability - Lenovo Support (US)*, http://support.lenovo.com/us/en/product_security/superfish (last visited Feb. 23, 2015).

> "Now injecting ads into a browser is bad enough, doing so by running an HTTPS proxy on the machine is a lot worse. HTTPS shouldn't be touched unless it is for a very good reason - inserting ads is never a good reason.
>
> But what makes it still orders of magnitude worse than that, is that their proxy uses the same certificate on all affected (or, perhaps more accurate, infected) PCs. Hence anyone can obtain the private key of the certificate - which, as people have already showed, isn't rocket science - and use this to man-in-the-middle HTTPS traffic without the Lenovo user being aware."[22]

44. Another expert said:

> "The latest Superfish debacle highlights the current strategy for device manufacturers across the electronics ecosystem looking to get their slice of the billion-dollar advertising revenue market that has made Google and others so successful. Unfortunately, like the case with Lenovo and many others, users' privacy and security are compromised - often in secret - leaving them extremely vulnerable to malicious hackers who leverage the this type of tracking technology against them."[23]

45. Even the United States government has determined that Defendants' Superfish Surveillance Software is a security threat. US-Cert, a website operated by the United States Computer Emergency Readiness Team, a division of the Department of Homeland Security, released an "Alert" on February 20, 2015 and warned:

> "Starting in September 2014, Lenovo pre-installed Superfish VisualDiscovery spyware on some of their PCs. However, Superfish was reportedly bundled with other applications as early as 2010. This software intercepts users' web traffic to provide targeted advertisements. In order to intercept encrypted connections (those using HTTPS), the software installs a trusted root CA certificate for Superfish. All browser-based encrypted traffic to the Internet is intercepted, decrypted, and re-encrypted to the user's browser by the application – a classic man-in-the-middle attack. Because the certificates used by Superfish are signed by the CA installed by the software, the browser will not display any warnings that the traffic is being tampered with. Since the private key can easily be recovered from the Superfish software, an attacker can generate a certificate for any website that will be trusted by a system with the Superfish software installed. This means websites, such as banking and email, can be spoofed without a warning from the browser."[24]

46. Ultimately, Defendants profited for months on the unauthorized acquisition and alteration of consumers' private internet communications. Undeniably, Defendants' methods demonstrate a wholesale disregard for consumer privacy rights and violate numerous federal laws.

---

[22] *Feedback Friday: Lenovo Preinstalled Superfish Adware on Laptops – Reactions | SecurityWeek.Com*, http://www.securityweek.com/feedback-friday-lenovo-preinstalled-superfish-adware-laptops-%E2%80%93-reactions (last visited Feb. 23, 2015).

[23] *Id.*

[24] *Id.*

FACTS RELATING TO PLAINTIFF HUNTER

47. On October 6, 2014, Plaintiff Hunter purchased a Lenovo Y50 laptop from Lenovo.com and paid $1,951.38 after tax. Unknown to Plaintiff at the time he ordered it, his Lenovo Y50 laptop was secretly bundled with Defendants' Superfish Surveillance Software.

48. As soon as Plaintiff received his laptop in the mail, on or about October 10, 2014, he began using his computer and connected it to a local wireless network and the internet. Plaintiff has since regularly used the laptop to browse the internet, send and receive emails, shop online, and conduct online banking.

49. On February 20, 2015, Plaintiff Hunter was alerted by news reports stating that the Superfish Surveillance Software was likely installed on his laptop. Once he confirmed that the Superfish Surveillance Software was present on his laptop, Plaintiff searched online on how to remove it and the Superfish Root Certificate and did just that.

50. Thus, from on or about October 10, 2014 to February 20, 2015, the Superfish Surveillance Software was operating on his computer, intercepting all of his internet traffic, and attempting to inject (and actually injecting) unwanted advertisements into his browsing sessions.

51. Plaintiff never agreed to any terms or conditions regarding the Superfish Surveillance Software, nor was he aware that the Lenovo laptop he purchased would contain the Superfish Surveillance Software. Accordingly, Plaintiff never consented to Defendants' monitoring of, access to, and/or interception of his internet communications.

CLASS ALLEGATIONS

52. Plaintiff David Hunter brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of himself and the following Class:

> All individuals in the United States who purchased a Lenovo computer with the Superfish Surveillance Software pre-installed on it and who connected the computer to the internet.

53. The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the

Defendants or their parents have a controlling interest and its current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

54. **Numerosity:** On information and belief, hundreds of thousands of consumers fall into the definition of the Class. Members of the Class can be identified through Defendants' records, discovery, and other third party sources.

55. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff's claims are representative of the claims of the other members of the Class. That is, Plaintiff and each member of the Class purchased laptops that was preinstalled with the Superfish Surveillance Software and had their communications read and altered without consent. Plaintiff also has no interests antagonistic to those of the Class, and Defendants have no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to the Class.

56. **Typicality:** Plaintiff's claims are typical of the claims of other members of the Class, in that Plaintiff's and the members of the Class sustained damages arising out of Defendants' wrongful conduct.

57. **Commonality and Predominance:** There are many questions of law and fact common to Plaintiff's and the Class's claims, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a) whether Defendants intentionally designed their Superfish Surveillance Software to reroute and alter consumers' internet traffic;

b) whether Defendants intentionally installed an insecure root certificate that remains installed even after consumers remove Defendants' software;

c) whether Defendants' obtained consent before installing and operating their Superfish Surveillance Software;

d) whether Defendants' conduct described herein violated the Stored Communications Act (18 U.S.C. §§ 2701, *et seq.*);

e) whether Defendants' conduct described herein violated the Electronic Communications Privacy Act (18 U.S.C. §§ 2510–22.); and

f) whether Defendants have been unjustly enriched at the expense of Plaintiff and the Class.

58. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definition" based on facts learned through additional investigation and in discovery.

FIRST CAUSE OF ACTION
Violations of the Electronic Communications Privacy Act
(18 U.S.C. §§ 2510–22.)
(On Behalf of Plaintiff and the Class)

59. Plaintiff incorporates the forgoing allegations as if fully set forth herein.

60. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–22 ("ECPA") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. . . ." 18 U.S.C. § 2510(12).

61. By using the Superfish Surveillance Software to intercept and modify Plaintiff's and the Class's online browsing activity, Defendants endeavored to and did intercept communications between Plaintiff's and the Class's computers on the one hand, and the servers for the websites they browsed on the other.

62. Thus, Defendants intentionally obtained and/or intercepted, by device or otherwise, these electronic communications, without the knowledge, consent or authorization of Plaintiff or the Class.

63. Accordingly, Defendants' conduct violated 18 U.S.C. § 2511(1)(a) because they intentionally intercepted and endeavored to intercept Plaintiff's and Class members' electronic communications.

64. Defendants likewise violated 18 U.S.C. § 2511(1)(d) by intentionally using the contents of Plaintiff's and the Class's electronic communications (*i.e.*, their online browsing activity) that they intercepted using the Superfish Surveillance Software.

65. Plaintiff and the Class suffered harm as a result of Defendants' violations of the ECPA, and therefore seek (a) preliminary, equitable and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendants as a result of their unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

SECOND CAUSE OF ACTION
Violations of the Stored Communications Act
(18 U.S.C. §§ 2701, *et seq*.)
(In the Alternative to the First Cause of Action)
(On Behalf of Plaintiff and the Class)

66. Plaintiff incorporates the allegations contained in Paragraphs 1 through 58 as if fully set forth herein.

67. The ECPA broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. . . ." 18 U.S.C. § 2510(12). The Stored Communications Act incorporates this definition.

68. Pursuant to the ECPA and Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.* ("SCA"), "electronic storage" means any "temporary storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). This type of electronic storage includes communications in intermediate electronic storage that have not yet been delivered to their intended recipient.

69. The SCA mandates, among other things, that it is unlawful for a person to obtain access to stored communications on another's computer system without authorization.

18 U.S.C. § 2701.

70. Congress expressly included provisions in the SCA to address this issue so as to prevent "unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." S. Rep. No. 99–541, 35, 1986 U.S.C.C.A.N. 3555, 3589.

71. Defendants accessed facilities through which electronic communications services are provided through their Superfish Surveillance Software. Specifically, Plaintiff's and the Class's computers provide electronic communications services that include operating as printer servers and wireless networking providers (*e.g.*, with Bluetooth or WiFi), amongst others.

72. In addition, Plaintiff's and the Class's computers operated as remote terminals of third-party facilities through which electronic communications are provided. Modern web applications communicate in near real-time over the internet, meaning that when Plaintiff and the Class access such web applications by visiting web pages, their internet browsers act as portals to the facilities that provide electronic communications services, such as electronic bulletin boards, electronic mail servers, and computer server centers.

73. Through the Superfish Surveillance Software, Defendants accessed Plaintiff's and the Class's web browsing communications (*i.e.*, their browsing activity) while those communications were in temporary storage on their laptop computers.

74. Accordingly, Defendants violated 18 U.S.C. § 2701(a)(1) by accessing without authorization facilities through which an electronic communication service is provided (*i.e.*, web services connected to Plaintiff's and the Class's computers), and obtaining and altering their web browsing communications.

75. Further, Defendants violated 18 U.S.C. § 2701(a)(2) by exceeding the scope of any authorization granted to access Plaintiff's computers and thereby obtaining and altering their web browsing communications.

76. Additionally, Defendants have violated 18 U.S.C. § 2701(a)(2) because they intentionally exceeded authorization to access consumers' communications and obtained,

altered, or prevented authorized access to a wire or electronic communication while in electronic storage by their continued modification of users' secure internet connections, even after users uninstalled the Superfish Surveillance Software. Defendants had actual knowledge of, and benefited from, this practice.

77. Because Defendants programmed the Superfish Surveillance Software to operate for profit on Plaintiff's and the Class members' computers, they had knowledge of, and benefitted from, their unlawful conduct.

78. As a result of Defendants' conduct described herein and its violation of § 2701, Plaintiff and the Class have suffered injuries to their privacy rights, and economic harm due to Defendants' unjust enrichment at their expense. Plaintiff, on behalf of himself and the Class, seeks an order enjoining Defendants' conduct described herein[25] and awarding them the maximum statutory and punitive damages available under 18 U.S.C. § 2707.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

79. Plaintiff incorporates the allegations set forth in Paragraphs 1 through 65 as if fully set forth herein.

80. Plaintiff and members of the Class conferred a monetary benefit on Defendants. Defendants received and retained money by selling to their customers and business partners data collected from Plaintiff's and the Class members' computers through their Superfish Surveillance Software and/or by selling advertisements that were injected into Plaintiff's and the Class's web browsers. The advertisements were injected and all of the information was collected from Plaintiff and the Class without authorization and through deceptive business practices.

81. Additionally, Plaintiff and the Class members conferred a monetary benefit on Defendant Lenovo through the purchase of their Lenovo computers.

[25] To date, Plaintiff's recovery hard disk, which he paid for as a part of the purchase price of his Lenovo Y50 laptop, is still infected with the Superfish Surveillance Software and cannot be altered by Plaintiff. As such, Plaintiff requires an injunction to compel Defendants to replace his recovery hard disk with a version that does not contain the Superfish Surveillance Software.

82. Defendants appreciate or have knowledge of such benefit, as demonstrated by their public representations regarding the monetization of Plaintiff's and the Class members' online consumer activity.

83. Under principles of equity and good conscience, Defendants should not be permitted to retain the money obtained by selling information about or advertisements to Plaintiff and members of the Class, which Defendants have unjustly obtained as a result of their unlawful actions.

84. Accordingly, Plaintiff and the Class seek full disgorgement and restitution of any money Defendants have retained as a result of the unlawful and/or wrongful conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, pray for the following relief:

A. Certify this case as a class action on behalf of the Class defined above, appoint David Hunter as class representative, and appoint his counsel as class counsel;

B. Declare that Defendants' actions, as described herein, violate the Electronic Communications Privacy Act (18 U.S.C. §§ 2510–22), and the Stored Communications Act (18 U.S.C. §§ 2701, *et seq.*), and constitute unjust enrichment;

C. Award injunctive and other equitable relief as is necessary to protect the interests of the Plaintiff and the Class, including, *inter alia*: (i) an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein; (ii) requiring Defendants to delete their Superfish Root Certificate and Superfish Surveillance Software from infected computers and their recovery disks; and (iii) requiring Defendants to conspicuously and truthfully display the manner in which they collect and share data about monitored consumers.

D. Award damages, including:

i. the greater of (a) the sum of actual damages suffered plus any profits Defendants earned through their unlawful conduct, and (b) the greater

of $100 per Class Member, per day of Defendant's violations, or $10,000 per Class Member, pursuant to 18 U.S.C. § 2520(c)(2);

ii. the greater of (a) the sum of actual damages suffered plus any profits Defendants earned through their unlawful conduct, and (b) $1,000 per Class Member; and

iii. punitive damages where applicable, to Plaintiff and the Class in an amount to be determined at trial;

E. Award Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Award Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Award such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: February 23, 2015

Respectfully Submitted,

DAVID HUNTER, individually and on behalf of a class of similarly situated individuals,

By: /s/ Samuel M. Lasser
One of Plaintiff's Attorneys

Samuel M. Lasser (SBN – 252754)
slasser@edelson.com
Edelson PC
1934 Divisadero Street
San Francisco, California 94115
Tel: 415.994.9930
Fax: 415.776.8047

Rafey S. Balabanian*
rbalabanian@edelson.com
Benjamin H. Richman*
brichman@edelson.com
J. Dominick Larry*
nlarry@edelson.com
Amir C. Missaghi*
amissaghi@edelson.com
Edelson PC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

**Pro hac vice* admission to be sought.

Attorneys for Plaintiff and the Putative Class